INTERNATIONAL STANDARD

ISO 20078-1

Road vehicles — Extended vehicle (ExVe) web services —

Part 1:
Content

Véhicule routiers — Web services du véhicule étendu (ExVe) —

Partie 1: Contenu

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso .org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 31, *Data communication*.

A list of all parts in the ISO 20078 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

General

This document was developed to address the needs of different parties to access data, aggregated information and functionality (Resources) from Connected Vehicles in a standardized, safe and secure way. A framework is defined for interoperable web services used by several parties via the internet by adapting current and widely used IT approaches based on OAuth 2.0 (see ISO 20078-3).

As personal data protection rights are becoming stronger in several countries, this document also defines and recommends by its design, common methods to handle data protection and data privacy issues when accessing personalized vehicle data, information or functionality via web services.

This solution is supported by the fact that Vehicle Manufacturers (VM) by design and in factory more and more include telematics support for their vehicles, making vehicle data, information and functionality available at their VM backend system. Thus, instead of installing additional third party telematics equipment in the vehicle to achieve intended service goals, the already existing infrastructure can be (re-)used via interoperable web services. Such web services allow a third party to (re-)use the infrastructure in same manners as the VM uses it.

NOTE   Web service interfaces have been available and have been offered by VMs previously to this document but lack of standardization over the VMs, especially on authentication and authorization, led to the fact that third parties accommodate and design for several different VM implementations.
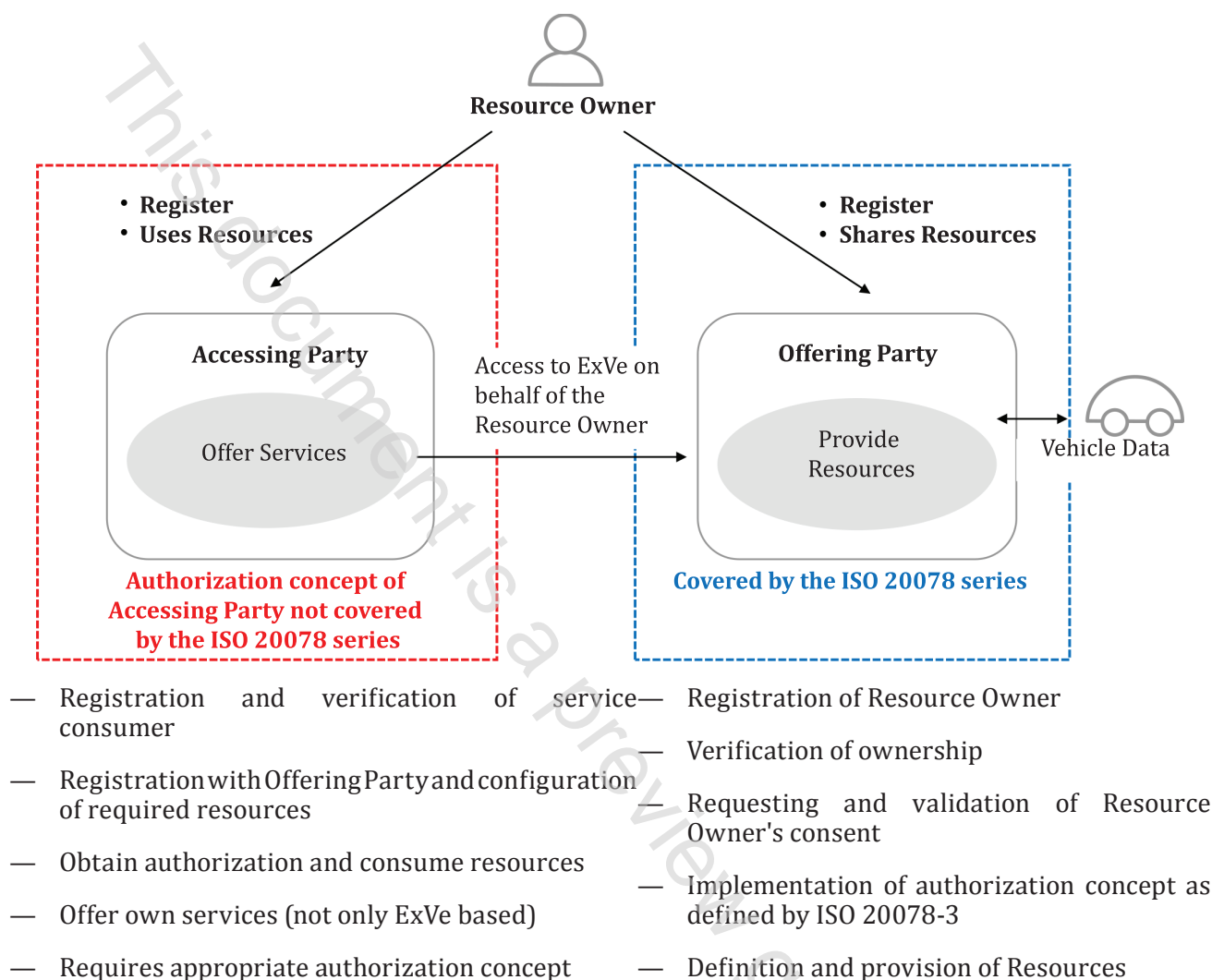
— Registration and verification of service consumer

— Registration with Offering Party and configuration of required resources

— Obtain authorization and consume resources

— Offer own services (not only ExVe based)

— Requires appropriate authorization concept

— Registration of Resource Owner

— Verification of ownership

— Requesting and validation of Resource Owner's consent

— Implementation of authorization concept as defined by ISO 20078-3

— Definition and provision of Resources

Figure 1 — Vision of the ISO 20078 series to standardize IT over the telematics backend

The authorization concept described by ISO 20078-3 covers only the authorization domain of the Offering Party; not the authorization domain of the Accessing Party. If an OAuth-compatible framework (see ISO 20078-3) is used to provide authorization by the Offering Party, three roles are technically mandatory:

— An Identity Provider; validates the identity of the Resource Owner;

— An Authorization Provider; manages the consents (grants) of the Resource Owner;

— A Resource Provider; shares Resources, depending on the consent of the Resource Owner.

The Access to Resources (data, aggregated information, and functions) cannot be authorized without validation of the Resource ownership and validation of the given consent of the Resource Owner. For registration, identity validation, and management of the Resource Owner an Identity Provider is used.

The Offering Party controls the Access to different Resources (URIs; see ISO 20078-2 Access) dependent on the availability of the Resource Owner's consent and owner's verification status. As such, the role of the Authorization Provider is required.

The Resource Provider exposes the actual Resources (via URIs; see ISO 20078-2) and enforces the Authorization Policy defined by the Authorization Provider.

The Accessing Party as a consumer of the Resources obtains Authorization from the Authorization Provider in order to access URIs (see ISO 20078-2). This requires:

— The registration of an Accessing Party as an ExVe client of the Offering Party;

— Configuration of required Resources (URIs) and may be providing intended purpose of use;

— Requesting Access to pre-configured Resource Groups and/or Containers.

The Accessing Party offers its own independent services based on the shared Resources (data, aggregated information, and functions). These Accessing Party services may depend on additional Resources and not only — per se — the Extended Vehicle Resources.

The Authorization domains of Accessing and Offering Parties are different, and the Accessing Party requires its own appropriate authorization concept (e.g. an additional Accessing Party Authorization Provider, if the OAuth 2.0 framework is also applied technically at the Accessing Party). Such Accessing Party authorization concepts are not in scope of ISO 20078-3 and held open.

Overview of the ISO 20078 series

This document states the minimum requirements, recommendations, permissions and external constrains for ensuring interoperable web services from an Accessing Party's perspective. The document:

— states requirements on the structure and format of Resources;

— contains guidelines on how to define the unique Resources of an individual application;

— defines the entities and roles, necessary for granting an Accessing Party Access to Resource Owner's Resources;

— states requirements on how an Accessing Party accesses Resources, including requirements on how to use the defined and referenced technologies, see Table 1.

The above-mentioned requirements and guidelines areas are addressed in the ISO 20078 series.

The ISO 20078 series is applicable for any application or service that intends to use web services.

The ISO 20078 series does not cover requirements for specific applications, resource definitions or XML/JSON schemas. These need to be described in the specific application or use case; e.g. see ISO 20080 Remote Diagnostics Support.

To elaborate more, this document defines all entities and roles that are used over in the ISO 20078 series. It standardizes how an Offering Party defines Resources. Depending on Resource category the Offering Party uses different kind of identifiers. Such Resources can be exposed directly or through Containers. It also describes different ways of representing Resources in web services, such as XML and JSON.

ISO 20078-2 defines the usage of a common communication protocol that enables Access to Resources (URIs), thereby standardizing how an Accessing Party can Access Resources via Web services of an Offering Party, using Hypertext Transfer Protocol (HTTP) over Transport Layer Security (TLS); i.e. HTTP Secure (HTTPS). The Representational State Transfer REST is selected for using a common way to represent data, aggregated information, and functions (Resources) [ISO 20078-2].

ISO 20078-3 standardizes the security model of the web service, including different roles and entities involved in an Authorization Policy. Three roles are defined: Identity Provider, Authorization Provider and Resource Provider at the Offering Party. Additional roles are the Accessing Party and the Resource Owner. The Resource Owner is in charge of its Resources. The role model is defined as a reference implementation of *OAuth 2.0* and *OpenID Connect 1.0* compatible frameworks [ISO 20078-3].

ISO /TR 20078-4 summarizes this document, ISO 20078-2, and ISO 20078-3 by *logical processes* for the displaying the interaction of all defined roles and entities[1]. The processes define the needs for a registration, authentication, and authorization of an Accessing Party. For granting, denying and

revoking Access to Resources, processes involving the Resource Owner are defined. The Resource Owner is generally in charge of those processes, which may depend on certain use case. However, these processes allow for a full self-determination of the Resource Owner on sharing Resources to Accessing Parties.

The ISO 20078 series defines in general a framework based on the communication and authorization protocols listed in from Table 1. Those technologies can be used for implementation of individual web services to share Resources and, therefore, allow for any service or application implementation on the Accessing Party domain.

In this document, entities are defined as the fundamental objects that represent, for example — vehicles, ECUs, drivers and fleets, and servers at an IT backend. Roles are defined as a grouping of entities and have relationships that allow for an interaction; e.g. The "Offering Party" (IT backend) offers Resources (ECU data) to an "Accessing Party" (service implementer).
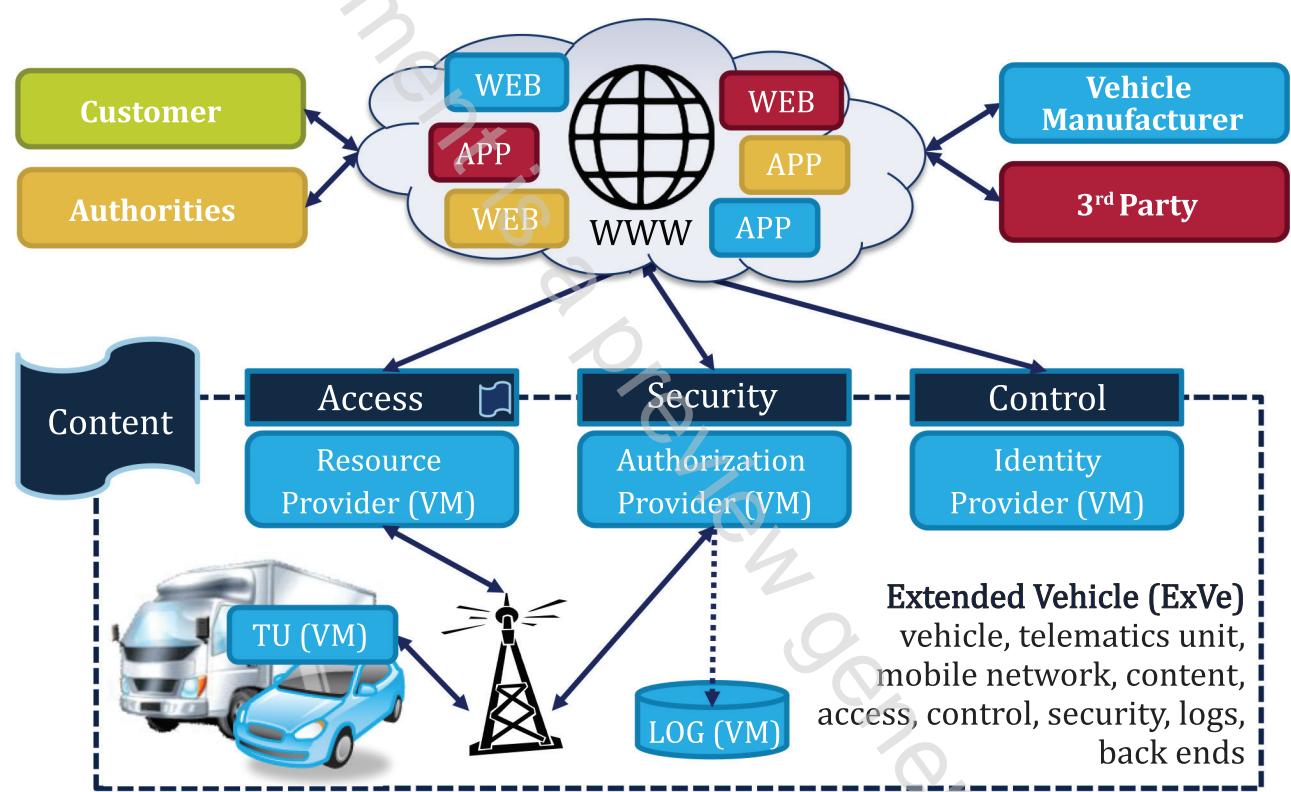
ISO 20078-1 Content	TU — vehicle integrated telematics unit
ISO 20078-2 Access	LOG — records access, events, failures, and intrusions
ISO 20078-3 Security	APP & WEB — application & web services
ISO/TR 20078-4 Control	Stakeholders — customer, authorities, VM, 3rd party

Figure 2 — Schematic presentation of the vision of the ISO 20078 series

ExVe web services are comprised of road vehicles combined with the telematics backend system of the Vehicle Manufacturer (the "Offering Party"), mainly acting as a Resource provider. This enables for a 3rd party, as well as the Vehicle Manufacturer, mainly acting as a service/application provider (the "Accessing Party") to access offered Resources via the internet; see Figure 2.

The concept of Containers is also introduced which allows an Accessing Party to specify what Resources it wants to access. Containers are a recommended solution where (data) privacy by design applies.

Logging (LOG of Figure 2) is an important part of any IT solution. It is, however, not considered within the scope of the ISO 20078 series due to potentially strong dependencies on certain IT backend infrastructures.

JSON (in addition to XML and Key-Value listing) is recommended for representation of Resources (URIs).

Table 1 — List of used information technologies

Transport Protocol	HTTP 1.1 (or later version) over TLS 1.2 (or later version)
Service Design	RESTful
Data format	JSON (recommended)
	XML
	Key-Value
Authorization	An OAuth 2.0 (or later version) compatible framework
End User Authentication	An OpenID Connect 1.0 (or later version) compatible framework

Road vehicles — Extended vehicle (ExVe) web services —

Part 1:
Content

1 Scope

This document defines the different concepts, entities and roles involved in implementing and delivering ExVe web services. In addition, it also gives an overview of the necessary activities that should be executed by the different roles involved and a logical order for those activities.

This document defines the concept of identifiers (direct and correlated), different Resource categories (e.g. personal, vehicle related, pseudonymized and anonymized Resources) and different approaches on how to bundle sharable Resources (e.g. Resource Group or Container).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 20078-2, *Road vehicles — Extended vehicle (ExVe) web services — Part 2: Access*

ISO 20078-3:—[1)], *Road vehicles — Extended vehicle (ExVe) web services — Part 3: Security*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1 Roles and entities

3.1.1
Vehicle Manufacturer
VM
company manufacturing road vehicles

3.1.2
Connected Vehicle
road vehicle that is enabled for communication over a Wide Area Network (WAN)

Note 1 to entry: A WAN can, for example be defined as a nationwide mobile phone network with a corresponding backend (server) architecture.

---

1) Under preparation. Stage at the time of publication: ISO/FDIS 20078-3:2019.